



SAN BERNARDINO: Supervisors appoint Oscar Valdez to controller position

By [ALEJANDRA MOLINA](#)

2016-02-17 18:17:31



The San Bernardino County Board of Supervisors appointed Oscar Valdez to fill the auditor-controller/treasurer/tax collector position after Larry Walker announced his retirement from the post in January.

In a special meeting Wednesday, Feb. 18, the Board of Supervisors unanimously voted 5-0 to appoint Valdez, who currently serves as the county assistant auditor-controller/ treasurer/tax collector.

The county charter requires supervisors to appoint someone to serve the remainder of Walker's term, which expires in 2018. The position becomes effective March 5.

Valdez, who works under Walker, said at the meeting he was "honored and humbled" by the supervisors' decision.

"I will make sure this department is run with integrity ... clear transparency and efficiency," Valdez told the supervisors.

Valdez also noted his mother's sacrifice in immigrating from their native Mexico for opportunities in the U.S.

"I've really lived the American Dream," he said.

Supervisor James Ramos, who chairs the board, said 17 people applied to the position. Five of the nine qualified applicants were interviewed, he added.

Ramos said Valdez understands the complexities in San Bernardino County.

"Being familiar with what it is that the county, not only now, but in prior year's budgets is going through, brought that expertise to us," Ramos said.

Contact the writer: 951-368-9462 or amolina@pe.com

© Copyright 2016 Freedom Communications. All Rights Reserved.
[Privacy Policy](#) | [User Agreement](#) | [Site Map](#)

San Bernardino County Sun (<http://www.sbsun.com>)

San Bernardino County supervisors appoint new auditor-controller/treasurer/tax collector

By Joe Nelson, The Sun

Thursday, February 18, 2016



Succeeding longtime San Bernardino County Auditor-Controller/Treasurer/Tax Collector Larry Walker could be an intimidating prospect for some, but Oscar Valdez said he is ready to take the helm when Walker retires March 5.

“I feel I’m up to the challenge right now to fill those shoes. I definitely appreciate his leadership,” Valdez, the county’s assistant auditor-controller/treasurer/tax collector since 2011, said of Walker after the Board of Supervisors unanimously appointed him as Walker’s successor during a special meeting Wednesday.

Walker announced last month he would be [retiring](#) after 18 years as auditor-controller. He previously held the additional titles of county recorder and county clerk, and since 2010, has also served as county treasurer and tax collector after those offices were merged with the auditor-controller’s office.

In his 38 years of public service in San Bernardino County, Walker, a Chino resident, also served as a county supervisor and mayor of Chino.

After reviewing 17 applicants, which were then whittled down to five top candidates, board Chairman James Ramos and Vice Chairman Robert Lovingood — who served as a two-man committee, reviewing applications and interviewing applicants — recommended Valdez for the job.

They cited his extensive background and experience as a county administrator and his familiarity with the county’s budget, its technologies and partner agencies.

Valdez, who attended Wednesday’s meeting with his wife, Beatriz, and their two children, Joanna, 16, and Jonathan, 12, in tow, addressed the board after its vote, vowing to run the office with “integrity, independent judgment, transparency and efficiency.”

Valdez said he began his career with the county auditor-controller’s office in 2000. In 2006, he went to work for county Treasurer-Tax Collector Dick Larsen. After the treasurer-tax collector’s office merged with the auditor-controller’s office in 2010, Valdez was promoted to assistant auditor-controller/treasurer/tax collector.

Valdez said Walker is leaving his elected office in top form.

“I think he’s definitely left a solid foundation of upper management. We have a very strong team,”

By [Shea Johnson](#)[Print Page](#)

February 17, 2016 4:22PM

San Bernardino County Supervisors eye own plan before DRECP

SAN BERNARDINO — Two desert conservationists welcomed a resolution passed Wednesday by San Bernardino County Supervisors that essentially highlights the Bureau of Land Management's vow to collaborate on a major renewable energy plan.

In a special session, the board unanimously voted to establish a position on the BLM's proposed land use plan amendment in Phase 1 of the Desert Renewable Energy Conservation Plan.

The BLM released its final Environmental Impact Statement in November, outlining its strategy for 10 million acres of federal public lands in the Southern California desert. The move signaled the wind down of the first of three phases for the massive initiative, which will ultimately cover 22 million acres in the state's desert — more than half of which is in San Bernardino County.

But county leaders, not thin on outstanding concerns, reiterated notice Wednesday that they will finish work on their own Renewable Energy Element before recommending alignment revisions to the land use plan amendment pertaining to DRECP's first phase. Officials say their ability to fully evaluate the BLM plan thus far has been "constrained" by the county's in-progress element, which still must face extensive public involvement.

The resolution Wednesday calls attention to the BLM's commitment to amend its land use plan to "match the County's objectives and land use designations."

In a February 2015 position paper, the county expressed concerns over utility-scale renewable energy development near unincorporated communities and rural areas.

Neil Nadler, member of the Alliance for Desert Preservation, and Lorrie Steely, founder of Mojave Communities Conservation Collaborative, both commended the board's resolution Wednesday.

Speaking about rural communities that could be affected by large-scale industrial development, Steely said her appearance in front of the board was to show "resounding support for the action you're taking."

In November, several wildlife groups praised the BLM's federal lands blueprint as successfully marrying conservation, recreation and renewable energy. But others were skeptical if the outline had evolved enough to mitigate issues raised since the first draft of the DRECP was released in September 2014.

Shea Johnson may be reached at 760-955-5368 or SJohnson@VVDailyPress.com. Follow him on Twitter at [@DP_Shea](#).

<http://www.vvdailypress.com/article/20160217/NEWS/160219764>

[Print Page](#)

San Bernardino County Sun (<http://www.sbsun.com>)

San Bernardino County fire agencies to be outfitted with ballistic vests, helmets

City to manage equipment grant for county fire for active shooter situations

By Sandra Emerson, Redlands Daily Facts

Wednesday, February 17, 2016

San Bernardino County fire agencies will be getting ballistic vests and helmets.

The Redlands City Council on Tuesday night authorized the city's Fire Department to manage a grant that would fund the purchase of the equipment for the county's fire agencies. The equipment will help protect personnel as they provide emergency care to victims during an active shooter incident.

"This grant has no matching requirement and the city can expect full reimbursement within 30 days of our completion of requisite paperwork," Fire Chief Jeff Frazier said to the council Tuesday night.

The San Bernardino County Operational Area Approval Authority initiated a multiyear Homeland Security Grant Program-funded effort to provide protective equipment to fire and rescue personnel who routinely respond to active shooter incidents, according to the staff report.

The authority includes fire, law, emergency management and public health representatives who coordinate funding for individual agency projects and regional programs, according to the report.

"The fire service is evolving. We are an all-risk organization and with that we're responding to different types of events up to and including these active shooting events that are happening nationwide," acting San Bernardino City Fire Chief Tom Hannemann said. "We're very appreciative and supportive of the fact that we are able to get our allotment of ballistic vests and helmets. It's not enough to outfit the entire department, but it's a start."

The authority allocated \$301,956 to purchase the equipment for fire and rescue agency personnel, requiring that one jurisdiction be responsible for managing the purchase.

The Redlands Fire Department volunteered to manage the grant.

With the funding, 138 units of body armor and 276 ballistic plates will be purchased through the state's contract with Safariland LLC and 138 ballistic helmets will be purchased through the city of Fontana's contract.

Redlands will spend \$301,956 for the gear but will later be reimbursed with grant funding, according to the staff report.

"It goes along with our mutual-aid, with the regular county support, and it's one way we can leverage and buy at an economical basis and get reimbursed for it," Redlands Councilwoman Pat Gilbreath said Tuesday. "We're just a temporary banker, if you will."

Hannemann said he hopes to purchase more equipment in the near future, but along with the equipment

comes training.

Hannemann said San Bernardino City Fire participated in an active shooter training at Indian Springs High School in San Bernardino about three years ago with agencies from Loma Linda, Redlands, Colton, Rialto, San Bernardino County Sheriff's Department and the San Bernardino City Unified School District, which proved beneficial in responding to the Dec. 2 shooting at the Inland Regional Center in San Bernardino.

"There were a lot of lessons learned that we overcame at the Dec. 2 event, and I think that was one of the reasons why we had such a successful outcome at that event," he said.

URL: <http://www.sbsun.com/government-and-politics/20160217/san-bernardino-county-fire-agencies-to-be-outfitted-with-ballistic-vests-helmets>

© 2016 San Bernardino County Sun (<http://www.sbsun.com>)

Sources: Grand Jury Witnesses Threatened With Prosecution

Tonight new sources go on the record alleging that witnesses called to testify have been threatened.

By: [Gina Silva](#)

POSTED:FEB 17 2016 09:29PM PST

UPDATED:FEB 17 2016 10:48PM PST

Fox 11 News has exposed one case after another of children beaten, tortured, and left to die in abusive homes in our ongoing series, *The Children Are Dying*. Our sources say many of those children would be alive today if the San Bernardino County Department of Children and Family Services had done its job.

We told you about a County Grand Jury investigation into these deaths, and about the whistleblowers who risked their livelihood by coming forward to tell us about their concerns. Six months later, new sources tell us that top San Bernardino County officials have been intimidating jurors and witnesses and threatening them with prosecution, if they don't back away from investigating CFS. "They've infiltrated the Grand Jury and now they're telling the Grand Jury what to investigate, what not to investigate, and that's not the purpose of the Grand Jury.

The Grand Jury is supposed to be an independent oversight of county operations when concerns are made," says one of our sources. Another tells us, "The ones that were investigating the Department of Children and Family Services knew that they were on to something. They did not want to back down and, before you know it, the grand jury legal advisor has threatened them with potential lawsuits if they print something that is considered defamation." The legal advisor they are referring to is Deputy District Attorney Michael Dauber. He declined an interview with Fox 11 News, saying he couldn't answer questions because of Grand Jury confidentiality laws.

San Bernardino County District Attorney Mike Ramos did sit down for an interview with us. He denied all of the allegations made against the legal advisor who reports to the D.A.'s office. During the interview, reporter Gina Silva asked him about the new allegations, "Telling witnesses that they can not reveal information because they could be prosecuted, is that something that a legal advisor should be doing?" Ramos responded, "That's not only something he shouldn't be doing, but he has not done it. That has not happened in a Grand Jury proceeding."

But attorney Valerie Ross, who represents a witness who testified before the County Grand jury, says the legal advisor did interfere with the Grand Jury investigation. Ross says, "I got a call from the legal advisor who told me that if my client testified, he'd be committing a crime." Ross says the legal advisor did not elaborate, but she took the warning seriously and told her client to leave the Grand Jury immediately. "My conclusion was there was an effort to interfere. A witness doesn't usually get in trouble for answering a Grand Jury's question. A witness gets in trouble for failing or refusing to answer a question," says Ross.

Perhaps most disturbing is the allegation that a lead juror was removed from the Grand Jury because he refused to stop investigating CFS *and* he was suspected of being one of our sources. D.A. Ramos had this to say, "As far as the individual that was removed, that's a decision that's made by a Superior Court judge, the presiding judge." A disheartened source says, "The report will come out that the county has cleaned up its act, that there's no more issues."

Meanwhile, our sources say, the problems with CFS continue. "There hasn't been any change. We're still having children dying at alarming rates. We're still having children left in homes where they should be removed." Ramos says our sources should take their evidence to him, so *he* can launch an investigation. "If they really want us to take a look at it, they need to come to me, come to my office," says Ramos. But that's not something these sources are comfortable doing. They say their only hope now is for an outside agency like the State Attorney General's Office or the FBI to investigate San Bernardino County.

Copyright 2016 [FOX 11 Los Angeles](#) : [Download our mobile app](#) for [breaking news](#) alerts or to watch FOX 11 News | Follow us on [Facebook](#), [Twitter](#) and [YouTube](#).



SAN BERNARDINO: Photographer captured the lives of city's African Americans

By [SUZANNE HURT](#)

2016-02-15 17:09:32



For more than half a century, African American photojournalist Henry Hooks documented the diversity of San Bernardino.

He pushed to get the black community into the city's newspapers starting in the 1940s – providing shots to the San Bernardino Sun and the San Bernardino Telegram without pay or a photo credit.

"I was just glad to get minority pictures in the paper," Hooks said. "There was no one like me showing up in the paper."

From 1946 until 2004, his cameras gave him access to photograph influential African Americans visiting the area and local movers and shakers – from the campaigning Rev. Jesse Jackson, who was the second African American to run for president, and actress Ruby Dee to California's first black school district superintendent, Dorothy Inghram.

Hooks also captured generations of people and events that shaped African American history in the city, largely through his role as a staff photographer for the black-owned Precinct Reporter.

To mark Black History Month, 100 of his photos are on exhibit at the San Bernardino County Museum in Redlands. "Community Chronicles: Photographs by Henry Hooks" runs through Feb. 28.

The Louisiana native became obsessed with photography at age 13. He won a 120-mm box camera by sending a boxtop coupon in to a Joy toothpaste promotion.

In 1943, he came to Norton Air Force Base and was a projectionist showing training films for the Army Air Corps during World War II. He later became a civilian missile systems inspector based at Norton.

Retiring in 1979, he began covering social and political events for the Precinct Reporter full-time until retiring a decade ago.

A classy, engaging professional, he photographed the national NAACP convention in Los Angeles – capturing then-Virginia Gov. Douglas Wilder, the first African American governor since Reconstruction, meeting local NAACP leader Willie Clark, Precinct Reporter Publisher Brian Townsend said.

"Not only could he frame a picture, but he could take over the scene and get the picture he wanted to get," Townsend said.

Hooks captured church socials, weddings, debutantes, entertainers, politicians and families celebrating milestones in the community or the custom-built studio at the back of the yellow stucco house where he lives with wife Opal, 92, within view of the San Bernardino mountains.

Last week, he pointed to photos lining walls and sitting on shelves in his old studio and talked about the many faces he's photographed.

"This girl now is a pharmacist. He works at Cal State San Bernardino. These girls here were going to be the

Supremes,” said Hooks, standing in a purple shirt and suspenders that match his brown pants.

Now 94, his hands still know every contour and knob on the large format Crown Graphic 4 x 5 camera sitting on a tripod in a corner. He pulled out what was once the top-of-the-line press camera and opened it.

He showed his photos of Colin Powell, who later became the first black U.S. secretary of state, and the late civil rights activist Rosa Parks, wearing a hat and scarf in a photo at an event whose significance has been lost to the passage of time.

“She was just like the girl next door. No air. No nothing. Just good people,” he said.

Hooks has diabetes and is going blind. He’s got implants in both eyes and can no longer drive.

Hooks hasn’t given up photography entirely – he takes photos of backyard roses and tomatoes with his iPhone. He misses getting out in the community to capture what’s going on.

“I’ve had a good life,” he said.

Contact the writer: 951-368-9444 or shurt@pe.com

© Copyright 2016 Freedom Communications. All Rights Reserved.
[Privacy Policy](#) | [User Agreement](#) | [Site Map](#)



Rancho Cucamonga Involves Spanish-Speaking Community Members in Strategic Planning

POSTED BY : [PUBLICCEO](#) FEBRUARY 17, 2016 IN [LOCAL GOVERNMENT](#)

Rancho Cucamonga's Spanish speaking residents had a lot to say about their community. Unfortunately, many of them were not confident enough to voice their concerns and engage in local government. These residents became distrustful of city government, primarily living in an underserved area which often faced disproportionate differences. A number of policies and programs that are developed and implemented affect this portion of the population, yet their input was not requested or incorporated into the solutions. The city of Rancho Cucamonga developed [Community Champions](#) to engage Spanish-speaking residents in a leadership program, providing them the opportunity to collaborate with the city to develop policies, programs, and strategies to improve the quality of life for their community.

No opportunities existed for the few residents who wanted to engage with city officials to raise their concerns. Many had never been to city hall, let alone a Rancho Cucamonga City Council meeting and did not know who their elected leaders were, or knew that their voice mattered.

Over one-third of the population in Rancho Cucamonga identifies as Hispanic. This population is at higher risk for various chronic diseases and resides in neighborhoods that are not easily accessible to a healthy lifestyle. Residents in the southwest portion of the city in particular faced many challenges to the quality and length of their life, with higher rates of poverty and fewer neighborhood amenities. Two out of every three residents were obese or overweight and three out of every four school children did not meet fitness standards. There were no outlets selling fresh produce, limited access to open spaces for exercise, and the streets lacked curbs, sidewalks, and bike lanes. Despite these inconsistencies, these populations are traditionally less represented in local decision making including city council meetings.

Rancho Cucamonga leaders strongly believe that local community members are best equipped to solve local issues. In order to do this, it was critical for Spanish-speaking residents to become actively engaged in community issues if the city was going to effectively improve the quality of life for its residents. To do this, it must give residents, especially those who are most disadvantaged, a voice to create the healthiest thriving community.

The city has a long history of civic engagement as the foundation of its governance style. Healthy RC is a city community partnership with over 75 community stakeholders, including elected officials, city staff, the county health department, hospitals, schools, nonprofits and community based organizations, faith based groups, businesses, local universities, residents, and youth collaborating to improve the quality of life through policies, programs, and partnerships.

LATEST HEADLINES

[Santa Clara County Opens Free 'Drug Donation' Pharmacy](#)

[Massive Public Works Project Will Help Clean Sacramento River](#)

[No running water and no solutions as California's driest county despairs](#)

[California Counts: What makes a person vote \(or not\)?](#)

[Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman](#)

[Click here for more headlines](#)

SIGN UP FOR OUR DAILY NEWSLETTER!

First Name

Last Name

Email Address *

[Sign Up](#)

Educate your staff to help protect kids!
Click here for Keenan's FREE Abuse Prevention resource today.

Keenan Associates

The idea of [Community Champions](#) was developed through the Healthy RC initiative to engage Spanish-speaking residents as leaders and partners who not only inform decisions and policies, but also play an active role in implementing and sustaining them. Participants work in partnership with local governmental leaders and officials, community partners, resident and youth groups to voice concerns and issues and identify and implement long-term policy driven solutions.

Community Champions meet bi-weekly to enhance their leadership and communication skills, deepen their understanding of public policy and local governmental processes, and build their capacity to plan and implement solutions to their identified priorities in their neighborhoods. They have increased access and availability to healthy food by dramatically rezoning where community gardens and farmer's markets could be located, simplifying the permitting process, and reducing associated fees.

Instrumental in identifying opportunities in the city that require additional attention, Community Champions have canvassed neighborhoods, collected data and conducted neighborhood assessments, engaged local residents, and applied for, and secured, grants to improve the quality of life for residents in this area. They have also conducted walkability assessments around local schools to gather data for successful Safe Routes to School infrastructure grant applications that created new sidewalks in their neighborhood enhancing safety and increasing walkability and bikability for students and their families.

Community Champions were successful in collaborating with the city and its Healthy RC stakeholders on the development of policies such as community gardens, farmer's markets, and complete streets. They not only advocated for the passage of these policies, but were actively involved in coordinating and conducting focus groups, comprehensive surveys, and drafting policy language and recommendations that were later adopted by the city council, often speaking in Spanish at city council meetings. As a result of their involvement, the Complete Streets policy was recognized as the 10th best Complete Streets policy in the nation.

The program has also received regional recognition. Recently, they were invited to speak to public health students at the University of Southern California on the importance of providing meaningful engagement opportunities to local residents.

By learning how to navigate through the policy process, the Community Champions are improving the dialogue with local decision makers, applying for grant opportunities, and making informed decisions that affect all residents, and particularly those in the southwestern area of the city.

Rancho Cucamonga's innovative approach provides a model for other local governments to partner with residents to create policies and programs that benefit the entire community. It is the city's commitment to engaging and empowering all residents in improving the quality of life for everyone who lives, works, and plays here that is the heart and soul of Rancho Cucamonga.

[Originally posted at the League of California Cities.](#)

Comments

0 comments



Contact ICFA today for a financing package tailored to your unique project.

- Affordable Housing
- Healthcare
- Utilities
- School Districts

ICFA is a California Joint Powers Authority

FOLLOW PUBLICCEO



2,962
Followers



0
Fans



Subscribe
Rss



**IMPROVE CITY SERVICES
WITH GUARANTEED RESULTS**



MUNISERVICES
Discover. Recover. Prosper.

Discover just how much revenue we can recover for your community.

Earn More

FREE
revenue assessment

GUTSY
Politics Getting in the Way of Governing?

Get to its Roots with
"GUTSY OPINIONS"

**No More Gridlock.
Just a Path to Progress.**

By [Shea Johnson](#)[Print Page](#)

February 17, 2016 5:07PM

Will celebrities flock to Adelanto medical marijuana industry?

ADELANTO — The budding medical marijuana industry that has been tied to a multi-million dollar rejuvenation in Adelanto could also become an enterprise for entertainers, City Councilman John "Bug" Woodard hinted at Wednesday.

Speaking as a guest on KCRW 89.9's "Press Play" with Madeleine Brand, Woodard said rapper Snoop Dogg would be a player in the city's cultivation industry and that singer Willie Nelson was also supposedly involved.

"They have a lot of people from the entertainment industry coming up here," he told Brand.

When reached by phone minutes after the broadcast, Woodard backtracked a bit, saying the information he had was "secondhand."

"I can't say too much about it," he said. "I can't divulge all that right now."

Adelanto spokesman Michael Stevens later said that Woodard heard about celebrities potentially entering into business in the city through developers who are directly involved with building facilities in the city's industrial parks, where zoning allows for the indoor grows.

A recent Orange County Register story on Adelanto's medical marijuana pursuit appeared to substantiate the entertainment industry angle, citing an attorney on one of the projects as saying one of Bob Marley's sons had signed on to license a strain of cannabis to be grown here.

There were also rumblings that Tommy Chong and Cypress Hill rapper B-Real have shown interest, the Register report said.

Meanwhile, Woodard told the radio station he met Snoop Dogg on Monday at a Grammys after-party.

Woodard also reiterated rallying messages for medical marijuana that have been voiced by officials throughout talks over the last year. He stressed that the industry's potential to lift the city out of a financial pickle is a far superior alternative to the 7.95-percent utility tax on residents that was meant to accomplish the same narrative. The tax was widely shot down by voters in November 2014.

Woodard said pharmaceutical companies had also become interested by the city's foray into medical pot.

Since three incumbents on the Council were ousted in November 2014 elections, the new-look leadership has been critical of former officials for not thinking outside the box when it came to generating revenue. Medical marijuana has been estimated by the Council as having the means to rake in millions of dollars into city coffers and a ballot measure to tax the facilities is expected this fall.

In late December, the city approved 25 medical marijuana permits. Only a few cultivators so far have moved forward with the next step: acquiring a conditional use permit. However, if all 25 proprietors were to ultimately open up shop, the industry would account for roughly 36 percent of all businesses in the city's three main industrial parks.

Shea Johnson may be reached at 760-955-5368 or SJohnson@VVDailyPress.com. Follow him on Twitter at [@DP_Shea](#).

<http://www.vvdailypress.com/article/20160217/NEWS/160219763>

[Print Page](#)

San Bernardino County Sun (<http://www.sbsun.com>)

Ontario goes upscale: Audi dealership coming to town

By Neil Nisperos, Inland Valley Daily Bulletin

Wednesday, February 17, 2016

ONTARIO >> An Audi dealership will be a new neighbor to QVC's under-construction distribution center, and city officials hope this is just the beginning of commercial development in the area.

Construction work is progressing toward a late summer opening for both the dealership and a [1 million-square-foot distribution facility for the QVC](#) home shopping network near the 10 Freeway and Archibald Avenue.

The dealership will employ about 60 to 70 people, and the QVC fulfillment center is expected to hire 1,000 employees.

[Walter's Audi](#), which has a location at the Riverside Auto Center, acquired 5 acres adjacent to the freeway last year. Company officials are in the process of acquiring another 3 to 4 acres west of its current construction site, according to Steve Kienle, principal of Walter's Audi.

The as-yet unfinished 50,000-square-foot dealership building already stands on the construction site. Kienle said the location with its excellent freeway visibility is "second-to-none."

"We're excited about the Ontario market," Kienle said. "It's a growing market with a lot of affluence. It's got old and new residents. People from Orange and Los Angeles (counties) are coming into the area. And when you look at the growth of Ontario, Rancho Cucamonga and Fontana, you can support another luxury car brand. That's why we're very excited about this."

Other luxury brands with dealerships in Ontario include Mercedes-Benz and BMW.

The land where both the dealership and QVC are planned was owned for about 50 years by the Meredith Family Trust and was considered one of the last undeveloped properties in Ontario. To the west of the dealership south of Inland Empire Boulevard and east of Vineyard Avenue, lies about 32 acres of vacant land zoned for commercial development.

"At this point, no other properties have been submitted for additional development, but we expect interested businesses will come as QVC opens up their operations, and Walter's opens up their operations. Those will be the catalyst for other development in the area," said John Andrews, economic development director for the city of Ontario.

The prime visibility of the developable land near the freeway will lead to more projects there in the near term, according to commercial real estate expert [Brad Umansky](#), CEO of the Rancho Cucamonga-based Progressive Real Estate Partners.

"It's very exciting to see (the formerly vacant Meredith property) being brought into productive use,"

Umansky said.

Andrews said the vacant land has the potential for all sorts of commercial uses, such as more car dealerships, retail and restaurants.

Kienle doesn't mind the prospect of competition.

"With more dealerships, you get synergy," Andrews said. "Across the freeway you have Mark Christopher (Auto Center), and for any auto dealership ... this would be a great opportunity to come in, build something from the ground up and have the visibility."

Ontario Councilman Alan Wapner is excited that new auto dealerships could put Ontario on the map as the prime center for automotive sales in Southern California.

"We're kind of creating a secondary auto center here," he said. "It's really exciting because Ontario's going to be known — and hopefully beat out Cerritos — as the No. 1 auto dealerships in California."

Staff writer Liset Marquez contributed to this report.

URL: <http://www.sbsun.com/business/20160217/ontario-goes-upscale-audi-dealership-coming-to-town>

© 2016 San Bernardino County Sun (<http://www.sbsun.com>)



CHINO HILLS: \$528.8 million Powerball jackpot unclaimed a month after draw

[STAFF AND WIRE REPORTS](#)

2016-02-17 11:58:29



A month after a lottery ticket worth \$528.8 million was sold at a Chino Hills 7-Eleven, its purchaser still has not come forward.

The ticket was one of three that matched all six winning numbers of the \$1.586 billion Powerball draw. The other tickets were purchased in Florida and Tennessee, and the winners have claimed their portions of the jackpot.

The purchaser of the Chino Hills ticket has a year to claim his or her prize. If the prize goes unclaimed, the money will be spent on California public schools.

If the winner does come forward, he or she will have an option of receiving the prize in a 29-year annuity, or a lump-sum payment of \$327.8

million before taxes.

A Florida couple was awarded their Powerball prize Wednesday.

Seventy-year-old Maureen Smith and 55-year-old David Kaltschmidt decided to take the lump sum payment of about \$327.8 million.

Kaltschmidt said at a news conference Wednesday they didn't inform family members until last week that they won.

The winning ticket was purchased at a Publix grocery store in Melbourne Beach.

John and Lisa Robertson of Munford, Tennessee, cashed in their ticket last month, also taking the lump sum.

The Chino Hills ticket earned a \$1 million payout for the 7-Eleven store's owner, Balbir Atwal. The Indian immigrant said he plans to share the winnings with family, friends, and store employees.

© Copyright 2016 Freedom Communications. All Rights Reserved.

[Privacy Policy](#) | [User Agreement](#) | [Site Map](#)

February 16, 2016

A Message to Our Customers

The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand.

This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake.

The Need for Encryption

Smartphones, led by iPhone, have become an essential part of our lives. People use them to store an incredible amount of personal information, from our private conversations to our photos, our music, our notes, our calendars and contacts, our financial information and health data, even where we have been and where we are going.

All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission. Customers expect Apple and other technology companies to do everything in our power to protect their personal information, and at Apple we are deeply committed to safeguarding their data.

Compromising the security of our personal information can ultimately put our personal safety at risk. That is why encryption has become so important to all of us.

For many years, we have used encryption to protect our customers' personal data because we believe it's the only way to keep their information safe. We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business.

The San Bernardino Case

We were shocked and outraged by the deadly act of terrorism in San Bernardino last December. We mourn the loss of life and want justice for all those whose lives were affected. The FBI asked us for help in the days following the attack, and we have worked hard to support the government's efforts to solve this horrible crime. We have no sympathy for terrorists.

When the FBI has requested data that's in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal.

We have great respect for the professionals at the FBI, and we believe their intentions are good. Up to this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to

create. They have asked us to build a backdoor to the iPhone.

Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.

The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.

The Threat to Data Security

Some would argue that building a backdoor for just one iPhone is a simple, clean-cut solution. But it ignores both the basics of digital security and the significance of what the government is demanding in this case.

In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.

The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable.

The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe.

We can find no precedent for an American company being forced to expose its customers to a greater risk of attack. For years, cryptologists and national security experts have been warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data. Criminals and bad actors will still encrypt, using tools that are readily available to them.

A Dangerous Precedent

Rather than asking for legislative action through Congress, the FBI is proposing an unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority.

The government would have us remove security features and add new capabilities to the operating system, allowing a passcode to be input electronically. This would make it easier to unlock an iPhone by "brute force," trying thousands or millions of combinations with the speed of a modern computer.

The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.

Opposing this order is not something we take lightly. We feel we must speak up in the face of what we see as an overreach by the U.S. government.

We are challenging the FBI’s demands with the deepest respect for American democracy and a love of our country. We believe it would be in the best interest of everyone to step back and consider the implications.

While we believe the FBI’s intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect.

Tim Cook

Shop and Learn

Mac
iPad
iPhone
Watch
TV
Music
iTunes
iPod
Accessories
Gift Cards

Apple Store

Find a Store
Genius Bar
Workshops and Learning
Youth Programs
Apple Store App
Refurbished
Financing
Reuse and Recycling
Order Status
Shopping Help

For Education

Apple and Education
Shop for College

For Business

iPhone in Business
iPad in Business
Mac in Business
Shop for Your Business

Account

Manage Your Apple ID
Apple Store Account
iCloud.com

Apple Values

Environment
Supplier Responsibility
Accessibility
Privacy
Inclusion and Diversity
Education

About Apple

Apple Info
Job Opportunities
Press Info
Investors
Events
Hot News
Legal
Contact Apple

More ways to shop: Visit an [Apple Store](#), call 1-800-MY-APPLE, or [find a reseller](#).



SAN BERNARDINO SHOOTING: DA Ramos, victims' attorney to weigh in on Apple court case

By [BRIAN ROKOS](#)

2016-02-17 14:33:34



San Bernardino County District Attorney Mike Ramos said Wednesday, Feb. 17, that he plans to join state and national district attorneys associations in filing a friend-of-the-court brief supporting the FBI's attempt to have Apple unlock the iPhone controlled by San Bernardino shooter Syed Rizwan Farook.

[Apple CEO Tim Cook said Wednesday that his company](#) will fight a federal magistrate judge's order requiring the electronics giant to cooperate with federal authorities, who are trying to determine whether anyone conspired with Farook and wife Tashfeen Malik on the Dec. 2 shooting that killed 14 people and wounded 22 at the Inland Regional

Center.

Apple is concerned that opening a so-called backdoor into a cell phone or tablet could have privacy consequences for other users.

"I think that if ever there was an exception to the rule, this is it," Ramos said. "We're talking about victims in my county who have lost loved ones who actually continue to fear for their lives, want to know if they were targeted, whether or not there are any others out there."

"And to not allow the FBI to get into this one phone I think is a huge public safety issue for all Americans," Ramos said.

Ramos said he expects this case to go all the way to the U.S. Supreme Court.

"It's going to be a fight. But I'll tell you this, I'm ready to fight. This is a fight that needs to be won. I'm not going to sit back and let them keep victims, or future victims, in the dark."

Ramos called Apple's opposition to Tuesday's court ruling "a slap in the face to our victims."

A friend-of-the-court brief, officially known as an amicus curiae, is usually filed by a party that is not directly involved in a case of public interest such as civil rights or privacy but still could be affected by a ruling. Such briefs often seek to raise awareness about some aspect of a case that the judge might otherwise miss.

Former U.S. District Judge Stephen G. Larson, founding partner of Larson O'Brien in Los Angeles, is filing such a brief to weigh into the Apple case on behalf of San Bernardino victims and family members.

Larson is also a former federal prosecutor who for several years worked with Eileen M. Decker, the U.S. Attorney for the Central District of California, who successfully sought the court order against Apple. Larson said he also is friends with Ramos. Decker and Ramos sought him out to file the brief, Larson said.

"The victims have the greatest interest of all in finding out why this terrible event took place and what our government and law enforcement can do to bring everyone involved in this to justice and ensure the best that we can something like this never happens again," Larson said.

“Part of that is understanding what happened, and why,” said Larson, who grew up and still lives in San Bernardino County. “This is one of the most significant terrorist incidents to have happened on American soil, and the fact that it happened here in our community is of grave concern to all of us.”

Larson said he is not charging the victims to represent them.

© Copyright 2016 Freedom Communications. All Rights Reserved.

[Privacy Policy](#) | [User Agreement](#) | [Site Map](#)



SAN BERNARDINO SHOOTING: DA to join FBI-Apple case amid safety, privacy debate

By [BRIAN ROKOS](#)

2016-02-17 14:33:34



San Bernardino County District Attorney Mike Ramos said Wednesday, Feb. 17, that he plans to join district attorneys associations in filing a friend-of-the-court brief supporting the FBI's attempt to force Apple to hack the county-owned iPhone controlled by San Bernardino shooter Syed Rizwan Farook.

Ramos called Apple's opposition to Tuesday's ruling that ordered Apple to assist the FBI "a slap in the face to our victims."

The DA's comments came as Inland residents weighed the competing interests of public safety and public privacy.

Apple CEO Tim Cook said Wednesday that his company will fight a federal magistrate judge's order requiring the electronics giant to cooperate with federal authorities, who are trying to obtain emails, text message and phone numbers from the device. They want to determine whether anyone conspired with county health inspector Farook and wife Tashfeen Malik on the Dec. 2 shooting that killed 14 people and wounded 22 at the Inland Regional Center.

Farook and Malik were killed in a subsequent gun battle, and the FBI has been unable to break the encryption of the phone it seized in a search.

Apple is concerned that opening a so-called backdoor into a cell phone or tablet could have privacy consequences for other users.

"I think that if ever there was an exception to the rule, this is it," Ramos said. "We're talking about victims in my county who have lost loved ones who actually continue to fear for their lives, want to know if they were targeted, whether or not there are any others out there."

"And to not allow the FBI to get into this one phone I think is a huge public safety issue for all Americans," Ramos said.

San Jacinto resident James Godoy, whose wife, Aurora Godoy, died in the Dec. 2 shooting, said Apple should be compelled to cooperate with the FBI.

"The government taps into stuff as it is," Godoy said. "Why can't they do it with Apple? It sounds kind of odd. Who does it hurt? Nobody."

But Karen Fagan, ex-wife of shooting victim Harry "Hal" Bowman, said the FBI's request is going too far.

"I know that it is a tempting argument to say that we should allow government access to private information in order to make people feel safe. After all, the argument goes, people who aren't breaking the law have nothing to hide. While that may be true, American citizens have been granted privacy rights, and this request breaches those rights," Fagan said.

'IT'S GOING TO BE A FIGHT'

Ramos said he expects this case to go all the way to the U.S. Supreme Court.

"It's going to be a fight. But I'll tell you this, I'm ready to fight. This is a fight that needs to be won. I'm not going to sit back and let them keep victims, or future victims, in the dark," he said.

A friend-of-the-court brief, officially known as an amicus curiae, is usually filed by a party that is not directly involved in a case of public interest such as civil rights or privacy but still could be affected by a ruling. Such briefs often seek to raise awareness about some aspect of a case that the judge might otherwise miss.

Former U.S. District Judge Stephen G. Larson, founding partner of Larson O'Brien in Los Angeles, is filing such a brief to weigh into the Apple case on behalf of San Bernardino victims and family members.

Larson is also a former federal prosecutor who for several years worked with Eileen M. Decker, the U.S. Attorney for the Central District of California, who successfully sought the court order against Apple. Larson, who grew up in San Bernardino County and still lives there, said he also is friends with Ramos. Decker and Ramos sought him out to file the brief, Larson said.

"The victims have the greatest interest of all in finding out why this terrible event took place and what our government and law enforcement can do to bring everyone involved in this to justice and ensure the best that we can, something like this never happens again," Larson said.

Larson said he is not charging the victims to represent them.

Godoy said data on Farook's iPhone could be helpful in explaining "some planning or motive" behind the terrorist attacks. He added the information may provide more evidence in the federal government's case against Enrique Marquez Jr., the 24-year-old Riverside man accused of supplying rifles and explosive powder used in the massacre.

"It's not like anybody is defending Apple's privacy," Godoy said. "Ideally, they should have done it on their own accord."

PHONE SECURITY IMPORTANT

Inland iPhone owners on Wednesday said they value their safety – but also their privacy.

Shortly after emerging from the Apple Store in Temecula, Kim Hyde, of Hemet, said this is a situation when the company should cooperate with the government.

"I just think that in the case of terrorism we have to band together against the terrorists," said Hyde, 48. "We have to do what it takes, whether or not it impinges on our civil liberties."

But Derek Drago, 44, of Murrieta, said he understands Apple's position.

"They want to have security for their customers, and that's the most important thing," said Drago.

Murrieta resident Mike Anderson, 64, who was shopping nearby at the Promenade mall with his wife, Kim, said he believes that people should dump their Apple products and boycott the company.

"If we could find more information on who else they were talking to, that would be awesome," said Kim Anderson, 58.

Monique Hayward, of Temecula, said she owns an iPhone and iPad Mini. As she stood on the sidewalk in front of the Apple Store, the 25-year-old health care worker conceded the government should be able to override privacy protections under special circumstances.

"I mean, I don't like the idea of someone being all in my phone," said Hayward. "But you never know – I could be a terrorist."

CALVERT: APPLE SHOULD COMPLY

At least one Inland congressman isn't too happy with Apple's intent to defy a court order to assist the FBI in unlocking the iPhone of San Bernardino shooter Syed Rizwan Farook.

"I don't know why there is a controversy, quite frankly," said Rep. Ken Calvert, R-Corona. "We've got 14 people

that are dead and we have a judge who's made an order and Apple should comply with it or be held in contempt."

"A dead person has no right or expectation to privacy," he added. "The FBI is not asking for the keys to the kingdom. They're simply asking Apple to unlock the phone to get to the facts to protect the public."

"... If this is their way of cooperating, God help us."

Rep. Pete Aguilar, D-Redlands, whose district includes the site of the terror attack, is urging Apple to cooperate with law enforcement.

"As the investigation into the attack at the Inland Regional Center continues, it's imperative that the technology community works with law enforcement and intelligence agencies to uncover critical information related to the terror attack," Aguilar said in a written statement.

"We must do everything in our power to learn more about how ISIS operates so we can destroy their system of recruitment and radicalization, and to prevent the violence we saw in San Bernardino from spreading to other communities throughout our nation."

In a statement, Rep. Paul Cook, R-Yucca Valley, said: "This is largely a matter for the courts at the moment, and I'm hopeful that Apple will find a way to continue cooperating with law enforcement."

COUNTY MAY REVIEW POLICY

County employees continue to use the phones issued to them, and they have the ability to configure security settings. Spokesman David Wert said the county could tell employees they can't create their own passcodes or cut off the iCloud, as Farook did, "but the county could not stop them from doing so. The county will most likely consider all of this as it reviews existing policies and creates new ones."

San Bernardino City Councilmember Fred Shorett said he is a strong supporter of privacy issues and the government staying out of business matters. He wondered Wednesday who would be trusted with the information that could be unlocked if Apple unwound the encryption that would erase data if too many wrong passcodes were entered.

"There's got to be a balance and there's got to be good judgment. ... I don't like the courts ordering a private-sector company what to do, but there's been a major crime committed here," Shorett said.

County Supervisor Josie Gonzales said it's important for the FBI to gain access to the phone but that further discussion is necessary before having Apple hack into the phone.

"It's not just about Dec. 2. There are millions and millions of people that would be impacted," she said.

Staff writers Stephen Wall, Alejandra Molina, Tom Sheridan, Jennifer Iyer and Jeff Horseman contributed to this report.

© Copyright 2016 Freedom Communications. All Rights Reserved.

[Privacy Policy](#) | [User Agreement](#) | [Site Map](#)



SAN BERNARDINO SHOOTING: Two families of victims divided on Apple rejection of FBI request

[STEPHEN WALL AND JENNIFER IYER](#)

2016-02-17 16:08:57



San Jacinto resident James Godoy, whose wife, Aurora Godoy, died in the Dec. 2 shooting at the Inland Regional Center in San Bernardino, said Apple should be compelled to cooperate with the FBI.

[Apple is resisting Tuesday's court order](#) that it assist the FBI in hacking into the county-issued iPhone of shooter Syed Rizwan Farook.

"The government taps into stuff as it is," Godoy said Wednesday, Feb. 17. "Why can't they do it with Apple? It sounds kind of odd. Who does it hurt? Nobody."

Godoy said data on Farook's iPhone could be helpful in explaining "some planning or motive" behind the terrorist attacks. He added the information may provide more evidence in the federal government's case against Enrique Marquez Jr., the 24-year-old Riverside man accused of supplying rifles and explosive powder used in the massacre.

"It's not like anybody is defending Apple's privacy," Godoy said. "Ideally, they should have done it on their own accord."

The ex-wife of another deceased victim, meanwhile, said she is concerned that the court might be jeopardizing iPhone users' privacy

rights.

Karen Fagan, of Upland, is the ex-wife of Harry "Hal" Bowman and mother of their two daughters.

"This is a very different thing than asking for data that is Apple's possession," Fagan wrote in an email. "They have complied with all of those requests. This is asking them to build a new piece of technology that could be used to invade the privacy of any iPhone. Furthermore, the FBI is citing an act written in 1789 (instead of new legislative action) to justify their request.

"I know that it is a tempting argument to say that we should allow government access to private information in order to make people feel safe. After all, the argument goes, people who aren't breaking the law have nothing to hide. While that may be true, American citizens have been granted privacy rights, and this request breaches those rights," Fagan wrote.

© Copyright 2016 Freedom Communications. All Rights Reserved.

[Privacy Policy](#) | [User Agreement](#) | [Site Map](#)

San Bernardino County Sun (<http://www.sbsun.com>)

San Bernardino shooting victim's father says Apple should cooperate with FBI

By Joe Nelson, The Sun

Wednesday, February 17, 2016

SAN BERNARDINO >> Gregory Clayborn, father of Sierra Clayborn, one of the county environmental health specialists killed in the Dec. 2 [mass shooting](#) in San Bernardino, said Wednesday he understands Apple Inc.'s position objecting to help the federal government unlock an iPhone used by gunman Syed Farook.

But given the circumstances, Apple should cooperate with the FBI, so long as it could do so without jeopardizing customer security and proprietary information, Clayborn said.

A U.S. magistrate [ordered Apple](#) on Tuesday to help the federal government hack into an encrypted iPhone belonging to Farook. The ruling requires Apple to supply highly specialized software the FBI can load onto Farook's county-owned work iPhone to bypass a self-destruct feature, which erases the phone's data after too many unsuccessful attempts to unlock it.

"It's one of those situations where they're trying to find out if other people were involved and if (Farook and Malik) were planning other attacks," Clayborn said. "I think Apple should help them. This warrants them helping and getting this situation resolved."

Apple CEO Tim Cook has [objected to the judge's order](#), saying it endangers privacy for millions of customers.

On Jan. 21, [claims](#) seeking more than \$200 million in damages were filed against the county on behalf of the Gregory Clayborn, his wife Kimberly - Sierra Clayborn's stepmother - and Tamishia Clayborn, Sierra's sister.

The Associated Press contributed to this report.

URL: <http://www.sbsun.com/general-news/20160217/san-bernardino-shooting-victims-father-says-apple-should-cooperate-with-fbi>

© 2016 San Bernardino County Sun (<http://www.sbsun.com>)



58°

SPONSORED BY



FOLLOW US

[Home](#) [News](#) [Sports](#) [Health](#) [Best Of: LA](#) [OC](#) [Eventful](#) [Video](#) [Audio](#) [Traffic](#) [Weather](#) [Directory](#) [Travel](#) [Deals](#) [Circulars](#) [Autos](#)
[Local](#) [Entertainment](#) [Business](#) [Politics](#) [Investigative](#) [Health](#) [Consumer](#) [National](#) [World](#) [Education](#)


Your living room. Our waiting room.



POWERED BY InQuicker

Expand +

Boyfriend Of San Bernardino Shooting Victim Says Apple Should Unlock Attacker's Phone

February 17, 2016 5:39 PM

Filed Under: [Apple](#), [Daniel Kaufman](#), [Inland Regional Center](#), [Ryan Reyes](#), [San Bernardino Shooting](#)

LISTEN LIVE



FOLLOW US ON

✉ [Sign Up for Newsletters](#)

SAN BERNARDINO (CBSLA.com) — After Apple said it [will not comply with a federal judge's orders](#) to help the FBI hack into an iPhone belonging to one of the killers in the San Bernardino shooting massacre, the boyfriend of one massacre victim said he strongly disagrees with the company and is considering getting rid of his Apple products.

Ryan Reyes, whose boyfriend Daniel Kaufman was killed in the terror attack, told CBS2's Crystal Cruz that the shooters are dead and therefore don't have rights. Reyes said he's considering getting rid of his Apple products.

The family of massacre victim Yvette Velasco also issued a statement criticizing "Apple's reluctance to cooperate with authorities."

"Frankly, it's difficult to understand why Apple would not jump at the opportunity to help uncover whatever information the phone may contain," the statement said.

"We're not talking about an ordinary case here; this is an act of terrorism, where 14 Americans lost their lives and many more were

BIG AIR
TRAMPOLINE PARK
REDLANDS, CA

YOUR COMMUNITY FAMILY FUN DESTINATION!

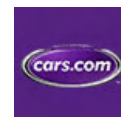
THURSDAY FAMILY NIGHT

Just: \$35

A FAMILY OF FOUR, RECEIVES ONE HOUR OF FREE JUMPING, PIZZA AND SODA FOR ONLY \$35!! SECOND HOUR OF JUMPING, ONLY \$7 EACH.

CLICK HERE!


Advertisements



- 1. [Look for the perfect car](#) 2 weeks ago [ad.doubleclick.net Cars.com](#) (sponsored) Compare top makes and models



- 2. [How Old Men Tighten Skin](#) 4 months ago

seriously injured. It's potentially a matter of [national security](#) , where other Americans' safety could be at risk."



MORE NEWS



Parents Voice Concerns Amid Court Order Mandating Release Of Student Information To



Judge: Apple Must Help FBI Hack San Bernardino Killer's Phone




Security Video Shows Woman Walking Into Subway Before Giving Birth In Restroom

Mandy Pifer, who was engaged to marry another victim of the attack, said she agrees.

"The little 'i' [in iPhone] could now stand for ISIS," she said. "Is my privacy important? Absolutely. But so is my life and my physical well-being and the well-being of my neighbors."

Many San Bernardino residents and others across the Southland agreed that Apple should comply with the court order.

"I think they should unlock it," said Crushunda Johnson, an Apple customer who lives in San Bernardino. "If there's any information that could stop something like this from happening again, that's something they should do."


The [government](#)  is asking the tech giant to disable the auto-erase feature, which wipes a phone's data if a phone's password is guessed incorrectly 10 times.

Some said Apple has a special obligation, since the FBI investigation could have national security implications.

"We've got to protect our country, and Apple should be forced to provide that information," said La Canada resident Jeff Peters.

RELATED: [San Bernardino Shooting Massacre](#)

But Apple has said it values the privacy of its customers above all else.

"We are challenging the FBI's demands with the deepest respect for American [democracy](#)  and a love of our country," Apple CEO Tim Cook wrote in a statement. "While we believe the FBI's intentions are good, it would be wrong for the government to force us to build a backdoor into our products."

"Ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect."

Many Apple customers in Pasadena said they support the company's stance in favor of maintaining customers' privacy.

"I do respect the fact that no matter who it is, they're going by what their policy is regarding privacy," said Chris Balan.

"If this is the stand we have to take to save a little bit of [privacy], I think maybe we should," said Valerie Main of San Gabriel.

"The government can want what the government wants, but Apple made a good decision in protecting our privacy," said Apple customer Warren Schenck.

According to Cook, Apple assisted the FBI in the days after the attack and has "worked hard to support the government's efforts to solve this horrible crime."

The FBI is still trying to piece together a 2-hour stretch between the massacre and the attackers' shoot-out with police. They're hoping recovering information from the iPhone could help fill in those gaps.

However, Apple says it does not have the software to comply with the court order, even if the company was inclined to do so.

"If they're saying they don't have the software to do it currently, I guess that could be a problem," said Glenn Willwerth, who owns a business in San Bernardino.

Apple has five days to appeal the federal judge's order.

 Comments

LOCAL / L.A. Now

In San Bernardino, where terrorists struck, residents debate FBI vs. Apple



Shown is a memorial for the victims of the Dec. 2 San Bernardino attack. Residents in and around San Bernardino had a mix of feelings Wednesday over Apple's refusal to comply with a federal court order to access data inside the smartphone used by the San Bernardino attackers. (Jay L. Clendenin / Los Angeles Times)

By **Paloma Esquivel** · Contact Reporter

FEBRUARY 17, 2016, 5:06 PM

The terrorist attack that left 14 people dead in San Bernardino in December changed Rudy Garcia's sense of the world. The San Bernardino resident was at work at a warehouse when police shot and killed the suspects in a shootout nearby. He heard the volley of gunshots inside.

"I feel like I'm not safe anymore. I don't trust anyone anymore," the 27-year-old said.

For him, the answer to a question debated Wednesday by technology experts, law enforcement and privacy advocates is clear. **Apple** must help the **FBI** access information from the shooters' cellphone.

"I think the FBI has to have the right so we can be safer," he said. "So nothing like that will ever happen again."

San Bernardino-area residents and those intimately affected by the shooting reacted on Wednesday with a mix of feelings to the announcement by Apple that it would oppose a federal court order to help the FBI access data on a cellphone used by one of the shooters in the Dec. 2. attack.

Some, including the father of one victim, said they hoped the two sides would find a way to balance the urgent need for information about the shooters with the privacy needs of ordinary cellphone users. Others urged the company to comply with the order and help law enforcement.

[See the most-read stories this hour >>](#)

Fourteen people were killed and 22 wounded when Syed Rizwan Farook and his wife, Tashfeen Malik, opened fire on a holiday gathering of county employees at the Inland Regional Center in San Bernardino.

Gregory Clayborn, father of Sierra Clayborn, a 27-year-old environmental health specialist who was killed in the attack, said he hoped Apple would be able to help law enforcement gain access to information from the phone without opening the doors too widely.

"This is just a specific incident," he said. "It's not like they have to have software to break everyone's codes for everyone that has an Apple phone. That's prying too deeply."

In a letter to customers, Apple Inc. CEO [Tim Cook](#) said the government had asked it "to build a backdoor to the [iPhone](#)."

"While the government may argue that its use would be limited to this case, there is no way to guarantee such control," Cook wrote.

Phyllis A. Muñoz, 62, who recalled how her office went on lockdown in the hours after the shooting and how she felt numb the day after, said she supported the FBI. Law enforcement urgently needs to know as much as possible about what happened, she said.

"They need to find out more," she said. "What [the shooters] did was awful."

She nodded across the road to a large memorial of flags, flowers and notes that still covers a corner sidewalk near the Inland Regional Center.

[See more of our top stories on Facebook >>](#)

At a San Bernardino Best Buy about a mile and a half from the site of the attack, where customers browsed a display of iPhones, several people agreed that the company should help access the data.

“Let’s say because they don’t get the information on the phone one person dies,” said Burton Rosenberg, 75, of Lake Arrowhead. “It’s an easy choice as far as I’m concerned.”

Aaron Winchester, 35, of Menifee, who wore an Apple Watch and carried an iPhone 6S Plus, said he bought the products because he felt they were more secure, and less prone to being hacked. Even so, he wants Apple to help law enforcement access the information.

“When it comes to terrorism,” he said, “if there’s information they can get that will help prevent future crimes, that’s in the best interest of everyone.”

Cielo Vargas, 69, of Green Valley Lake, an unincorporated mountain community in San Bernardino County, said she sympathized with the company.

“It’s a difficult situation for Apple because if they start giving out information anytime something happens, then people are not going to want to buy Apple. At the same time, if it helps find out something that’s going on,” she paused. “That’s hard. I’d hate to be in their position.”

In the end, though, she said the company should help.

“It’s lives you’re talking about,” she said. “I think they should allow it.”

For more Inland Empire news, follow me @PalomaEsquivel on Twitter.

MORE ON SAN BERNARDINO

Why Apple is battling investigators over San Bernardino terrorists' iPhone

Apple CEO Tim Cook explains why helping the FBI in terror phone probe is 'threat to data security'

After San Bernardino shooting, one doctor seeks ways to turn the 'golden hour' of treatment into minutes

Copyright © 2016, Los Angeles Times

This article is related to: [Apple Inc.](#), [FBI](#), [San Bernardino Terror Attack](#), [Apple iPhone](#), [Tim Cook](#)

San Bernardino County Sun (<http://www.sbsun.com>)

San Bernardino's IRC shooting investigation thwarted by Apple Inc.

By Joe Nelson, The Sun

Wednesday, February 17, 2016

An encrypted work-issued iPhone used by San Bernardino County employee and [Inland Regional Center gunman Syed Farook](#) is at the center of an imminent legal battle between Apple Inc. and the federal government.

[Apple CEO Tim Cook has vowed to fight a federal magistrate's order](#) help the FBI develop software known as a "backdoor" to bypass a four-digit numeric pass code that would unlock the iPhone 5C issued to Farook by the San Bernardino County Department of Public Health.

Cook said that once a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge. That could jeopardize the security of data stored on hundreds of millions of iPhones across the globe, he fears.

Despite the potential unintended consequences prompting Cook's reluctance, the U.S. Government argues that Farook is dead and the owner of the iPhone, the San Bernardino County Department of Public Health, has authorized the FBI to scrub the phone for evidence.

San Bernardino County spokesman David Wert said Wednesday the county is fully cooperating in the criminal investigation. He would neither confirm nor deny if investigators had reached out to the county since Magistrate Sheri Pym's ruling Tuesday. Wert declined to comment on Cook's opposition to the court order. "That's a matter between Apple and the FBI," Wert said.

Investigators have already dug up evidence in the iCloud account showing that Farook was in communication with some of the victims prior to [the mass shooting](#), and phone records revealed that Farook communicated with Malik using the iPhone in question, federal prosecutors said in their pleading.

In their motion to compel Apple to assist in unlocking the Farook's iPhone, federal prosecutors said the San Bernardino County Department of Public Health had a written policy that all digital devices issued to employees are subject to search at any time. Farook signed the policy as a condition of his employment, according to the court document.

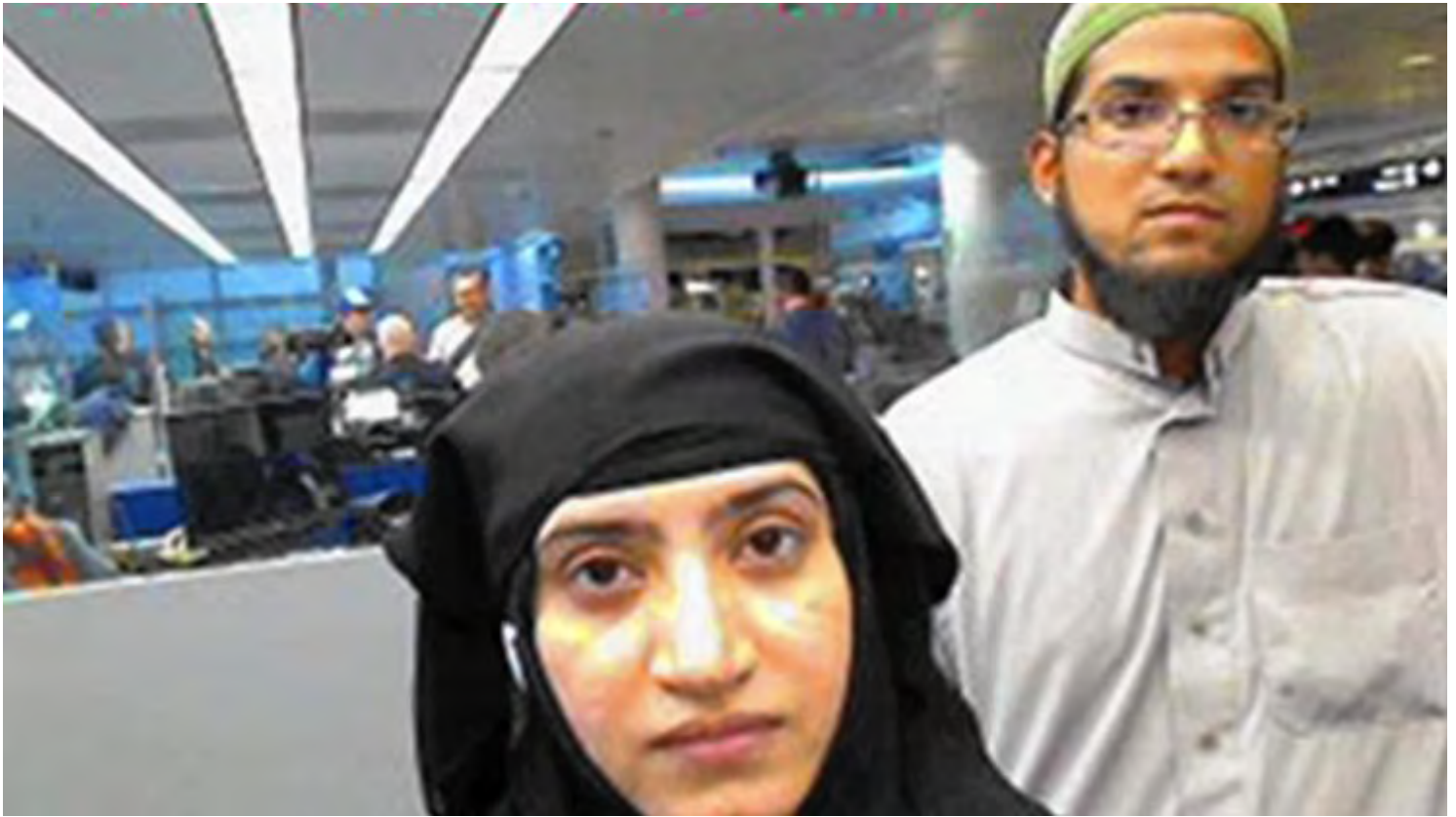
"It is worth noting as well that the user of the phone is now dead, the user was made aware of his lack of privacy on the work phone while alive, and the owner of the phone consents to both the search of the phone and to Apple's assistance in this matter," according to the court document.

URL: <http://www.sbsun.com/general-news/20160217/san-bernardinios-irc-shooting-investigation-thwarted-by-apple-inc>

© 2016 San Bernardino County Sun (<http://www.sbsun.com>)

LOCAL / CALIFORNIA

Apple CEO says helping FBI hack into terrorist's iPhone would be 'too dangerous'



Tashfeen Malik, left, and Syed Rizwan Farook killed 14 people in a shooting last year. The FBI is asking Apple to help hack into Farook's iPhone. (U.S. Customs and Border Protection)

By **Tracey Lien, Brian Bennett, Paresh Dave and James Queally** · **Contact Reporters**

FEBRUARY 17, 2016, 5:37 PM | REPORTING FROM SAN FRANCISCO

Setting up a pitched battle between Silicon Valley and the counter-terrorism community, Apple's chief executive said Wednesday that his company would fight a court order demanding the tech giant's help in the San Bernardino attack investigation, turning what had been a philosophical dispute into a legal skirmish that could have major ramifications for the tech industry.

Apple Inc. CEO Tim Cook said that the FBI request that the company develop software to hack into one of its own devices, an iPhone 5c, used by gunman Syed Rizwan Farook, would set a dangerous precedent that could compromise security for billions of customers. The government, Cook contends, is asking Apple to create a "backdoor" to its own security systems.

"Up to this point, we have done everything that is both within our power and within the law to help

them," Cook wrote in a letter published on the company's website. "But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create."

FULL COVERAGE: Terror attack in San Bernardino >>

The company will file an opposition to the court order, which was handed down in Riverside on Tuesday. The court order marks the first time Apple has been asked to modify its software to access data sought by the government, according to an industry executive familiar with the matter who spoke on condition of anonymity.

The Dec. 2 San Bernardino terrorist attack killed 14 people. Investigators said unlocking the phone could provide valuable information about the terror plot and whether Farook and his wife, Tashfeen Malik, received help from anyone else.

Chenxi Wang, chief strategy officer at the network security firm Twistlock, said the court battle would be a seminal moment in balancing "privacy and civil liberty against government data access."

"If Apple succeeds in fighting the court order, it will set up a high barrier for the FBI and the other government groups to access citizen data from now on," Wang said. "This will absolutely have a ripple effect. Apple is now viewed as the flag bearer for protecting citizen data, and if they succeed, there will be a flood of other companies following suit."

Tensions between tech magnates and Washington, D.C., have been high since the 2013 Edward Snowden leaks revealed a massive domestic spying network that left millions concerned about communications privacy. Apple also changed the way it manages phone encryption in 2014, making it nearly impossible for forensic investigators to sidestep its pass-code system. Previously, investigators could tap into a device's hardware port to access encrypted data, according to Clifford Neuman, director of USC's Center for Computer System Security.

The pass-code system is the key issue blocking federal investigators from gaining access to the data hidden on the phone used by Farook. Investigators want to unlock the phone by using a computer program to automatically guess numeric pass codes until one works, according to a court filing. But they say they require special access from Apple to attempt that on the phone without erasing data or getting bogged down in a long process.

Investigators say a feature is probably enabled that would immediately and permanently destroy encrypted data in the event of 10 consecutive failed log-in attempts.

Join the conversation on Facebook >>

In the government motion, the FBI argued that Farook intentionally disabled the phone's iCloud backup function six weeks before the Dec. 2 terror attack at the Inland Regional Center. Any communications linked to the shooting, as well as location data that might help the FBI map the movements of Farook and his wife before and after the attack, are accessible only through the phone itself, the government said.

Investigators were able to retrieve some data from previous iCloud backups, and companies like Apple normally comply with requests to retrieve cloud data because they do not involve giving the government access to company servers or altering software, Neuman said. The San Bernardino County Department of Health, which employed Farook, actually owned the device and gave the FBI consent to search it, according to court filings.

The court order handed down Tuesday would require Apple to provide the FBI with a "recovery bundle" or file that would reboot Farook's device while disabling the auto-erase feature. That would allow the FBI to repeatedly enter pass codes remotely without risk of destroying the data on the phone.

Robert Cattanach, a cybersecurity attorney and former Department of Justice special counsel to the secretary of the Navy, said the government's request leaves Apple in a difficult position as the company is thrust into the center of the battle to balance privacy needs against counter-terrorism efforts.

"The FBI's request ... represents the next step in the journey to find the Holy Grail of backdoor unencryption, and the next salvo in the ever-escalating battle between law enforcement and tech companies," Cattanach said.

In seeking this week's court order, the U.S. attorney's office cited the All Writs Act of 1789, a rarely used law that allows judges to issue orders they deem necessary and appropriate. Apple's argument that the government is overreaching has met favorable reception in at least one court.

Late last year, a U.S. magistrate in Brooklyn, N.Y., halted a government request to obtain a suspect's iPhone data in a drug conspiracy case, saying that the All Writs Acts might not provide enough legal foundation for such an order.

The Brooklyn magistrate hasn't issued a final order, but Apple told the court in a filing last week that it would like a decision because it has "been advised that the government intends to continue to invoke the All Writs Act ... to require Apple to assist in bypassing the security of other Apple devices in the government's possession."

Apple drew support from civil liberties advocates, who fear that totalitarian governments such as China will demand the company use a similar tool to open phones of opposition leaders and human rights activists.

"If the FBI can force Apple to hack into its customers' devices, then so too can every repressive regime in the rest of the world," ACLU staff attorney Alex Abdo said in a statement.

Apple's objection to the FBI's request may increase calls for a federal law that requires tech companies to design products that law enforcement officials can access with a search warrant. Earlier this year, a California legislator proposed a similar measure that would require all cellphones produced and sold in the state to have the capacity to be unlocked by law enforcement.

Any push for legislation would face stiff resistance from privacy advocates and technology companies, which say they are building products with encryption to protect users' privacy and data from hackers, and because customers want it.

Interested in the stories shaping California? Sign up for the free Essential California newsletter >>

The Obama administration, which has increasingly reached out to Silicon Valley over the last year, has not asked Congress to intervene in the hope that tech company executives would find a way to comply with search warrants while still protecting customers' privacy.

In the government's motion, the FBI asked Apple to create a software package designed to function only on Farook's phone. But Cook said in his letter that he was concerned about the potential for abuse.

"While the government may argue that its use would be limited to this case, there is no way to guarantee such control," he wrote.

Presidential candidates began weighing in on the issue Wednesday morning. GOP front-runner Donald Trump said he was floored that Apple had not volunteered to aid the FBI.

"Who do they think they are?" he asked on Fox News.

Speaking to reporters in South Carolina, Sen. Marco Rubio said he hoped the tech giant would voluntarily comply with the government's request, but acknowledged the court order is far from a simple issue.

In San Bernardino, locals reacted to news of Apple's refusal with mixed emotions. Some expressed concern about government overreach. But others sympathized with the FBI.

Aaron Winchester of Menifee, who wore an Apple Watch and carried an iPhone 6S Plus, said he bought the products because he felt they were more secure and less prone to being hacked. Even so, he wants Apple to help law enforcement access the information on Farook's phone.

"When it comes to terrorism," he said, "if there's information they can get that will help prevent future crimes, that's in the best interest of everyone."

tracey.lien@latimes.com | Twitter: @traceylien

brian.bennett@latimes.com | Twitter: @ByBrianBennett

paresh.dave@latimes.com | Twitter: @peard33

james.queally@latimes.com | Twitter: @JamesQueallyLAT

Lien reported from San Francisco, Bennett from Washington, D.C., and Dave and Queally from Los Angeles. Times staff writers Richard Winton and Joel Rubin in Los Angeles and Paloma Esquivel in San Bernardino contributed to this report.

MORE ON THE APPLE VS. THE FBI

How a passcode has foiled the FBI

The FBI wants Apple to pry into your iPhone

In San Bernardino, where terrorists struck, residents debate FBI vs. Apple

Copyright © 2016, Los Angeles Times

THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<http://www.wsj.com/articles/tim-cooks-dangerous-game-1455745398>

TECH | KEYWORDS

Apple CEO Tim Cook's Dangerous Game

The specifics of the fight over security are messier than Mr. Cook allows, and not all in Apple's favor



There is a risk that however this case turns out, Apple could lose a larger legal war. The Apple store on Fifth Avenue in New York. *PHOTO: ANDREW BURTON/GETTY IMAGES*



By

CHRISTOPHER MIMS

Updated Feb. 17, 2016 8:07 p.m. ET

Tim Cook is playing a dangerous game of brinkmanship with the U.S. government. In the process, he may set in motion political and judicial processes that will endanger the security of all our mobile devices.

First, let me say that I agree with the spirit of Mr. Cook's open letter rebuffing a

court order that Apple Inc. create a new version of the iPhone's operating system to allow the Federal Bureau of Investigation to access the locked, encrypted phone used by one of the assailants in the mass shooting in San Bernardino, Calif.

Mr. Cook asserts, correctly, that the FBI's request—for Apple to create new software that overcomes the phone's inbuilt security—is unprecedented. “We can find no precedent for an American company being forced to expose its customers to a greater risk of attack,” he wrote.

Here's the rub: The FBI says it wants Apple to create this software only for this one device. But if the code gets into the wild—and these things have a way of doing so—it will render the encryption on all iPhones everywhere essentially moot.

Still, the specifics of this case are messier than Mr. Cook allows, and not all in Apple's favor.

First, there are the optics of the situation: As tech analyst Ben Thompson notes, “It's a case of domestic terrorism with a clear-cut bad guy and a warrant that no one could object to, and Apple is capable of fulfilling the request.” Second, the iPhone in question is an older model iPhone 5C. It differs enough from newer iPhone models that, as developer and iOS security expert Dan Guido notes, Apple should technically be able to create for the FBI a solution that wouldn't endanger the security of newer iPhones.

Finally, there is a risk that however this case turns out, Apple risks losing a larger legal war. The fallout could force Apple—and others, including Google Inc. and Microsoft Corp.—to back down on their project of bringing strong encryption to everyday devices.

I am not a lawyer and this isn't an analysis of constitutional law, but some suggest that Apple is on the wrong side of legal precedent in its fight to protect devices from search with a warrant.

RELATED

- Apple Opposes Order to Unlock Phone Tied to Attack (<http://www.wsj.com/articles/apple-to-oppose-judge-order-to-help-unlock-phone-linked-to-san-bernardino-attack-1455698783>)
- Dispute Puts Focus on Centuries-Old Law (<http://www.wsj.com/articles/apples-iphone-dispute-with-government-puts-focus-on-centuries-old-law-1455739834?tesla=y>)
- The Debate: Privacy, Security and What's at Stake (<http://blogs.wsj.com/digits/2016/02/17/the-iphone-standoff-debate-privacy-security-and-whats-at-stake/>)

So to
sum
up,
Apple
is

publicly battling the FBI over protection of data in a grisly, high-profile case that would require the company to, at most, endanger the security of older model iPhones. The only logical explanation I can think of for why Apple might be standing on principle in this case is that it would set a precedent for future requests by law enforcement that could eventually lead to Apple's (and, frankly, consumers') worst nightmare.

That nightmare, which I wrote about previously, is a situation in which Apple is forced to build a security "back door" into all iPhones, the results of which are equivalent to removing encryption from the phones. Unless we want to make the financial, health and personal data of everyone with an iPhone available to cybercriminals, hackers and state actors, encryption back doors aren't something we as a civilization want to create.

Here, however, the FBI isn't asking for an encryption back door, at least not explicitly. Rather, it is asking for something more specific. And I worry that by so publicly refusing to cooperate, Apple is creating a situation in which eventually the courts or Congress will force it to do even more damage to the security of our most personal devices than capitulation in this case would require.

Write to Christopher Mims at christopher.mims@wsj.com

Copyright 2014 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.

San Bernardino County Sun (<http://www.sbsun.com>)

Apple is right: Judge's order would endanger everyone's personal data

Wednesday, February 17, 2016



A judge's order that Apple defeat the security system on one of its iPhones wouldn't amount to a mere slippery slope in terms of lost privacy and online security for the American public. It would be a water slide.

We all want to defeat terrorism. We want the FBI and other law enforcement agencies to catch the bad guys. If the misguided fools who carried out the terror attack in San Bernardino communicated with someone else about the attack, it would be good for the FBI to find that out.

But not so good that all Americans should surrender their most private information to the government — and in effect, to hackers and criminals.

Make no mistake. The “backdoor” way to defeat encryption that the judge asked Apple Inc. to provide in this one case would be used over and over again by law enforcement, any time an officer wants to have a look at a private citizen's data and can convince a judge — “just in case” the data might aid in an investigation somehow.

And that's only regarding well-meaning law enforcement. Much worse, the technique, if developed, would end up in the hands of every hacker and criminal who wants to grab your data in order to steal your money.

U.S. Magistrate Judge Sheri Pim issued an order Tuesday for Apple to provide “reasonable technical assistance” to help law enforcement agents retrieve data from the work phone of Syed Farook, the San Bernardino County employee-turned-terrorist who died, with his wife, in a shootout with police after [their attack left 14 dead on Dec. 2](#).

If Apple could do that in this one case and this one case only, that would be great. Law enforcement has clear legal reason to access the data on this phone. (That the terrorists destroyed their private phones after the attack, but not this work phone, makes it likely there's not much on it that would help the FBI, but that's beside the point.)

But what the judge asked is for Apple to defeat the “self-destruct” feature that wipes out data after 10 incorrect tries at the phone's passcode. Then the FBI could try passcodes in rapid succession until one works.

Undoubtedly Apple could do that, but it's doubtful it could do it for this one phone; such code likely would defeat the encryption feature of all iPhones.

That's why Apple CEO [Tim Cook posted a statement](#) saying his company would fight the order.

It's ludicrous to think such technology would never be used again. Remember the overreach of the National Security Agency in collecting phone records? Think the technology wouldn't fall into the hands of criminal hackers? Wouldn't it be used by repressive governments around the world to keep their citizens under control?

The judge's order says Apple may seek relief if it "believes that compliance with this Order would be unreasonably burdensome." Apple should fight it on that basis.

We're not trying to portray Apple as the saintly defender of privacy, freedom and apple pie. Its phones are programmed to allow the company to mine users' data for commercial purposes — many of its motives are suspect. But in this case, it's right.

That we're having this debate is a clear sign that we as a people already have been terrorized to the point that many are willing to give up our privacy and the safety of our personal information for false hopes of physical security.

Our voluntary surrender of our freedoms is exactly what the terrorists seek. If we do it, they win.

Fear should not push us that far.

URL: <http://www.sbsun.com/opinion/20160217/apple-is-right-judges-order-would-endanger-everyones-personal-data>

© 2016 San Bernardino County Sun (<http://www.sbsun.com>)



The New York Times | <http://nyti.ms/1KXszbO>

TECHNOLOGY

Apple's Stance Highlights a More Confrontational Tech Industry

Farhad Manjoo

STATE OF THE ART FEB. 17, 2016

The battle between Apple and law enforcement officials over unlocking a terrorist's smartphone is the culmination of a slow turning of the tables between the technology industry and the United States government.

After revelations by the former National Security Agency contractor Edward J. Snowden in 2013 that the government both cozied up to certain tech companies and hacked into others to gain access to private data on an enormous scale, tech giants began to recognize the United States government as a hostile actor.

But if the confrontation has crystallized in this latest battle, it may already be heading toward a predictable conclusion: In the long run, the tech companies are destined to emerge victorious.

It may not seem that way at the moment. On the one side, you have the United States government's mighty legal and security apparatus fighting for

data of the most sympathetic sort: the secrets buried in a dead mass murderer's phone. The action stems from a federal court order issued on Tuesday requiring Apple to help the F.B.I. unlock an iPhone used by one of the two attackers who killed 14 people in San Bernardino, Calif., in December.

In the other corner is the world's most valuable company, whose chief executive, Timothy D. Cook, has said he will appeal the court's order. Apple argues that it is fighting to preserve a principle that most of us who are addicted to our smartphones can defend: Weaken a single iPhone so that its contents can be viewed by the American government and you risk weakening all iPhones for any government intruder, anywhere.

There will probably be months of legal tussling, and it is not at all clear which side will prevail in court, nor in the battle for public opinion and legislative favor.

Yet underlying all of this is a simple dynamic: Apple, Google, Facebook and other companies hold most of the cards in this confrontation. They have our data, and their businesses depend on the global public's collective belief that they will do everything they can to protect that data.

Any crack in that front could be fatal for tech companies that must operate worldwide. If Apple is forced to open up an iPhone for an American law enforcement investigation, what's to prevent it from doing so for a request from the Chinese or the Iranians? If Apple is forced to write code that lets the F.B.I. get into the Phone 5c used by Syed Rizwan Farook, the male attacker in the San Bernardino attack, who would be responsible if some hacker got hold of that code and broke into its other devices?

Apple's stance on these issues emerged post-Snowden, when the company started putting in place a series of technologies that, by default, make use of encryption to limit access to people's data. More than that, Apple — and, in different ways, other tech companies, including Google, Facebook, Twitter and Microsoft — have made their opposition to the government's claims a point of

corporate pride.

Apple's emerging global brand is privacy; it has staked its corporate reputation, not to mention invested its considerable technical and financial resources, on limiting the sort of mass surveillance that was uncovered by Mr. Snowden. So now, for many cases involving governmental intrusions into data, once-lonely privacy advocates find themselves fighting alongside the most powerful company in the world.

"A comparison point is in the 1990s battles over encryption," said Kurt Opsahl, general counsel of the Electronic Frontier Foundation, a privacy watchdog group. "Then you had a few companies involved, but not one of the largest companies in the world coming out with a lengthy and impassioned post, like we saw yesterday from Tim Cook. The profile has really been raised."

Apple and other tech companies hold another ace: the technical means to keep making their devices more and more inaccessible. Note that Apple's public opposition to the government's request is itself a hindrance to mass government intrusion. And to get at the contents of a single iPhone, the government says it needs a court order and Apple's help to write new code; in earlier versions of the iPhone, ones that were created before Apple found religion on privacy, the F.B.I. may have been able to break into the device by itself.

You can expect that noose to continue to tighten. Experts said that whether or not Apple loses this specific case, measures that it could put into place in the future will almost certainly be able to further limit the government's reach.

That's not to say that the outcome of the San Bernardino case is insignificant. As Apple and several security experts have argued, an order compelling Apple to write software that gives the F.B.I. access to the iPhone in question would establish an unsettling precedent. The order essentially asks Apple to hack its own devices, and once it is in place, the precedent could be

used to justify law enforcement efforts to get around encryption technologies in other investigations far removed from national security threats.

Once armed with a method for gaining access to iPhones, the government could ask to use it proactively, before a suspected terrorist attack — leaving Apple in a bind as to whether to comply or risk an attack and suffer a public-relations nightmare.

“This is a brand new salvo in the war against encryption,” Mr. Opsahl said. “We’ve had plenty of debates in Congress and the media over whether the government should have a backdoor, and this is an end run around that — here they come with an order to create that backdoor.”

Yet it’s worth noting that even if Apple ultimately loses this case, it has plenty of technical means to close a backdoor over time. “If they’re anywhere near worth their salt as engineers, I bet they’re rethinking their threat model as we speak,” said Jonathan Zdziarski, a digital forensic expert who studies the iPhone and its vulnerabilities.

One relatively simple fix, Mr. Zdziarski said, would be for Apple to modify future versions of the iPhone to require a user to enter a passcode before the phone will accept the sort of modified operating system that the F.B.I. wants Apple to create. That way, Apple could not unilaterally introduce a code that weakens the iPhone — a user would have to consent to it.

“Nothing is 100 percent hacker-proof,” Mr. Zdziarski said, but he pointed out that the judge’s order in this case required Apple to provide “reasonable security assistance” to unlock Mr. Farook’s phone. If Apple alters the security model of future iPhones so that even its own engineers’ “reasonable assistance” will not be able to crack a given device when compelled by the government, a precedent set in this case might lose its lasting force.

In other words, even if the F.B.I. wins this case, in the long run, it loses.

Email: farhad.manjoo@nytimes.com; Twitter: [@fmanjoo](https://twitter.com/fmanjoo)

A version of this article appears in print on February 18, 2016, on page A1 of the New York edition with the headline: In This Standoff, Tech Firms Have a Long-Term Advantage .

© 2016 The New York Times Company



The New York Times | <http://nyti.ms/1oq2liH>

TECHNOLOGY

Explaining Apple's Fight With the F.B.I.

By **MIKE ISAAC** FEB. 17, 2016

Tuesday evening, a federal court ordered Apple to help the F.B.I. unlock an iPhone used by one of the attackers who killed 14 people in San Bernardino, Calif., in December.

Wednesday morning, Apple said in a strongly worded letter that it would challenge the court's request. While technology companies recently have resisted government demands, Apple's letter is one of the industry's most forceful pushbacks against a court ruling.

In the hours after Apple's letter was published, technologists and legal experts have been dissecting what, exactly, the Cupertino, Calif., company can't — or won't — do to help the government.

What is the government asking for?

The Federal Bureau of Investigation wants to examine the iPhone used by Syed Farook to determine whether he and his wife, Tashfeen Malik, had planned the shooting directly with the Islamic State. The iPhone, a 5c version

of the smartphone that was released in 2013, is locked by a passcode, which the F.B.I. wants Apple to circumvent. Apple would have to build a new version of its iOS smartphone software that allows the F.B.I. to bypass certain restrictions. Apple claims this software can give someone “the potential to unlock any iPhone in someone’s physical possession.”

So what does the court order require Apple to do?

The court is ordering the company to “bypass or disable” a feature that automatically wipes an iPhone clean of all its data after 10 incorrect password attempts have been entered. This is a standard feature on iPhones.

Technically, that would not require Apple to decrypt the passcode that blocks access by outsiders to the iPhone. It would allow the government to try an unlimited number of passwords without fear of the phone erasing all of its stored information.

In electronic security parlance, that is what is called a “brute force” attack, and all it takes is time and patience to submit a large number of passcodes. Brute force attacks are usually carried out with the assistance of a powerful computer, which can automatically input millions of different password combinations until it guesses the correct one.

Can Apple comply with the order if it wants to?

Apple’s opposition is mostly ideological.

“The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe,” Timothy D. Cook, Apple’s chief executive, wrote in the letter.

Apple argues that the software the F.B.I. wants it to create does not exist. But technologists say the company can do it.

Why can't the F.B.I. build this software?

The iPhone is designed to run only iOS software created by Apple. For the phone to recognize that the software was made by Apple, the company must sign each piece with an encrypted key to verify it. Even if the F.B.I. tried to build a new version of iOS, it would not have Apple's crucial signature.

The agency argues that this is a one-time request and wants Apple to create software only to get into Mr. Farook's phone, not unlimited access to iPhones everywhere.

Are there other ways for the F.B.I. to get this information?

There is a lot of data available that does not require Apple's assistance in unlocking the phone. The F.B.I. could ask Verizon, the cellular carrier by which Mr. Farook's phone was serviced, to give the agency more information on the phone.

The government could also request information from the application developers who created the apps for Mr. Farook's iPhone.

But those are avenues the F.B.I. has probably already pursued, explaining why it wants Apple to unlock the device. Some data is not accessible without Apple's intervention.

Are there other legal implications for the tech industry?

What Apple is most worried about is the precedent that compliance can set for future requests from the government. There are few earlier rulings courts can use for guidance, and Apple does not want to pave the road for similar requests to itself and other tech companies.

Other countries, like China, could also make similar demands.

"The key question here is how far can the government go in forcing a third

party to aid in surveillance?” said Christopher Soghoian, principal technologist for the American Civil Liberties Union.

Apple will most likely file an appeal with the court in the coming days.

A version of this article appears in print on February 18, 2016, on page B4 of the New York edition with the headline: Why Apple Is Putting Up a Fight Over Privacy With the F.B.I.

© 2016 The New York Times Company

How an Apple passcode has foiled the FBI



Apple has deterred hackers from making guesses. A security setting wipes an iPhone's data clean after 10 incorrect tries. (Carolyn Kaster / AP)

By **Paresh Dave** · Contact Reporter

FEBRUARY 17, 2016, 6:04 PM

Four numbers hardly seem like a foolproof way to protect a smartphone.

But that's likely what has stumped federal law enforcement, who have been unable to break into the iPhone 5C used by one of the San Bernardino shooters. That has led to a standoff between Apple and the FBI over the agency's right to access the device's contents — and its power to compel Apple to help it do so.

Password-protecting an iPhone seemed unnecessary in the early smartphone days, when most devices contained little more than contacts and music. But as smartphones evolved into powerful mini-computers storing troves of personal, location and financial data, the need to safeguard them has soared.

Phones today are better protected than they've ever been.

"You have to go out of your way to not have a passcode," said Eric Burger, director of the Georgetown University Center for Secure Communications. "We're much better off."

The increased use of passwords may be keeping out hackers or jealous boyfriends, but now authorities are finding themselves locked out, too.

The FBI's dilemma in the San Bernardino terror investigation has demonstrated how powerful these digital locks can be and could prompt more people to use them.

"The tools of the good guys have gotten a lot more powerful, stronger and with a lot more capability," Burger said.

The problem is the tools are available to everyone, including terrorists.

As smartphone theft blossomed worldwide, consumers were urged to turn on features enabling them to identify the real-time location of the phone and delete its contents over the Internet.

Smartphone makers even require a passcode, at minimum, if users want to use their phones as mobile wallets that store digital copies of credit cards.

"It's your banking information, who you had lunch with, where you've been," Burger said. "People are realizing criminals are using that information to clear out your bank account."

Apple added an extra layer of security in 2013 when it introduced Touch ID, a fingerprint scanner that allows users to unlock their phones by pressing their fingerprint to the home button.

Last year, Apple upped its security even more and remains the toughest device for outsiders to penetrate.

It increased the default passcode length to six characters from four, making them more difficult to crack.

[Join the conversation on Facebook >>](#)

Apple also has deterred hackers from making multiple guesses. A security setting wipes an iPhone's data clean after 10 incorrect tries.

That limit is what's stymieing FBI officials, who fear that if they keep trying to break into San Bernardino shooter Syed Rizwan Farook's iPhone 5C, they risk destroying all the content they're after.

Other smartphone companies have touted their phones' security options in recent years. Samsung's Knox feature locks data under a separate password into a harder-to-access layer of the smartphone. Microsoft pitches a phone to business customers that gives corporate officials new powers to secure employees' devices.

Cybersecurity experts applauded the efforts because in 2013 just 47% of U.S. adult Internet users locked their device in some fashion, according to a Consumer Reports survey. The numbers are much higher now, experts say.

"The real issue with security is still not so much about bits and bytes," Burger said. "It's about how to make it easier for users to use and help them understand why it's important."

Law enforcement has found ways around smartphone passcodes. Courts have regularly ordered Apple to turn over iPhone user data backed up on the cloud. And law enforcement authorities can exploit loopholes in Google's Android operating system to access data on phones running that software.

But "Apple is highly unique in the way it limits access to the area of the phone where information is stored," said Michael Harris, chief marketing officer at Guidance Software, a forensic software vendor.

That's what pushed the Silicon Valley giant to the center of the debate for a back door into smartphones.

Apple should have the capability to develop one, experts said, but the company's history with guarding consumers' data from outside entities shows it's probably headed in a different direction.

paresh.dave@latimes.com

Twitter: @peard33

FULL COVERAGE: Terror attack in San Bernardino >>

MORE ON APPLE VS. THE FBI

In San Bernardino, where terrorists struck, residents debate FBI vs. Apple

Court order in San Bernardino case could force Apple to jeopardize phone security

Editorial: The FBI wants Apple to pry into your iPhone

Copyright © 2016, Los Angeles Times

This article is related to: [Business](#)

THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<http://www.wsj.com/articles/newer-phones-arent-easy-to-crack-1455756764>

TECH

Newer Phones Aren't Easy to Crack

Fight around locked iPhone highlights growing role of encryption in digital life



Encryption scrambles smartphone data so that it is unreadable until unlocked with a unique key. *PHOTO: REUTERS*

By **JACK NICAS** and **ROBERT MCMILLAN**

Feb. 17, 2016 7:52 p.m. ET

The legal fight around the locked iPhone of one of the San Bernardino shooters highlights the growing role of encryption in digital life—and the intensifying battle between tech companies and the government over the proper bounds of the technology.

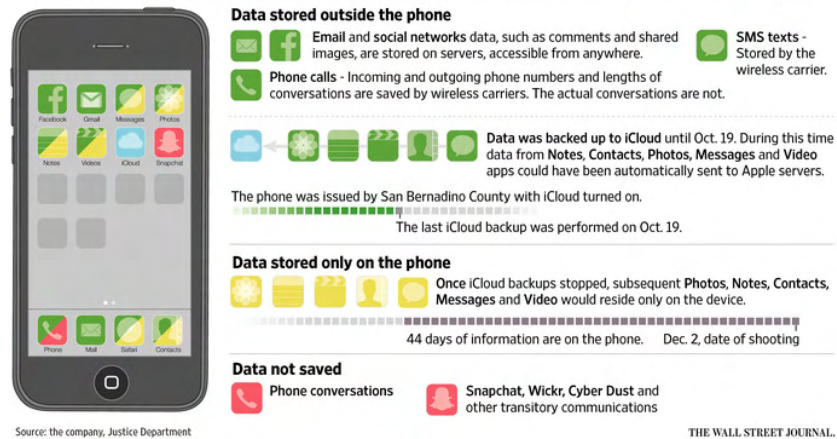
Encryption scrambles data so that it is unreadable until unlocked with a unique key. Apple Inc. and Alphabet Inc.'s Google thrust the issue into the spotlight in 2014, when they issued new versions of their software that automatically encrypted data stored on phones, such as contacts, photos and some text messages. Moreover, Apple and Google, which together power more than 90% of the world's smartphones, said they wouldn't be able to break the encryption codes themselves.

Law-enforcement officials, led by Federal Bureau of Investigation Director James

Comey, expressed alarm that encrypted phones could hamper criminal investigations. Such cases have been rare until now, because much of the data investigators seek can often be found elsewhere, such as call records maintained by telecom companies.

Desired Data, Within and Without

The FBI wants access to data on the iPhone 5C of shooting suspect Syed Rizwan Farook. Much of this data also exists outside the phone.



In the case of alleged shooter Syed Rizwan Farook, however, federal investigators say they have no other options. They persuaded a federal judge Tuesday to order Apple to circumvent the security measures on Mr. Farook's iPhone 5C, hoping to learn more about his contacts and communications in the final weeks of his life.

In essence, the government wants Apple to help it unlock the phone by trying every conceivable password. At the government's request, the judge ordered Apple to override the software that normally limits these attempts, such as a feature that erases all the data on the phone after 10 failed attempts.

Depending on the password that Mr. Farook used, there could be more than two billion combinations, which could take a computer 5½ years to try, Apple estimates. In a court filing, the Justice Department said it can't tell whether the auto-erase feature is enabled, "therefore trying repeated passcodes risks permanently denying all access to the contents."

Such a solution would be much harder on more modern versions of the iPhone, which ship with a cryptographic processor that makes the machine even harder to crack, said Dan Guido, head of Trail of Bits Inc., a security consulting firm that has studied the iPhone's design.

Had Mr. Farook used a phone running Google's Android operating system, assessing the encryption would be more complicated. That is because, unlike Apple, Google doesn't make most of the phones that use Android. Instead, there are more than 4,000 different Android devices made by more than 400 manufacturers, who use different flavors of Android.

Google has allowed Android users to encrypt a phone's contents since 2011, but many

haven't because it hurts the performance of older phones. In late 2014, Google began encrypting some phones by default with the release of Android version 5.0, dubbed Lollipop, including Google's flagship Nexus devices. But only about 35% of Android devices now run version 5.0 or higher, according to company data.

The Manhattan District Attorney's Office said in a November report that on some older Android phones, investigators know how to bypass passcodes. For some other Android devices, Google can reset the passcodes remotely, the report said.

Apple's and Google's smartphone encryption software apply to data stored directly on a device, and some communications, such as Apple's iMessage. Many messages sent and received on smartphones are stored elsewhere, such as Gmail correspondence retained on Google's servers.

The government hasn't specified the information it thinks may be on Mr. Farook's phone. In a court filing, an FBI agent said Apple, in response to a search warrant, had previously turned over data from the phone that had been backed up to Apple's iCloud service. That is another way in which investigators can often obtain information from encrypted phones.

But the agent said Mr. Farook had last backed up the phone on Oct. 19, about six weeks before the Dec. 2 shootings that killed 14 people. After that date, the agent said, Mr. Farook was believed to have communicated with his wife, and alleged accomplice, Tashfeen Malik, as well as several victims of the attacks.

Wireless carriers can access some standard text messages, and third-party apps, like WhatsApp, typically store users' correspondence.

Google says it provides users' Gmail messages when required under a court order. Google said that it received nearly 35,000 government requests for user data in 2014—up from 15,000 requests in 2010—and that it complies with the requests in about 65% of cases.

Write to Jack Nicas at jack.nicas@wsj.com and Robert McMillan at Robert.Mcmillan@wsj.com

Inland Valley Daily Bulletin (<http://www.dailybulletin.com>)

Why are Apple phones hard to crack?

By Staff and wire reports

Wednesday, February 17, 2016

WASHINGTON >> A U.S. magistrate judge has ordered Apple to help the FBI break into a work-issued iPhone used by Syed Farook, one of the gunmen in the [mass shooting](#) in San Bernardino. Apple CEO Tim Cook immediately [objected](#), setting the stage for a high-stakes legal fight between Silicon Valley and the federal government.

• Why do the Feds want the information off the phone?

Prosecutors say they think the device could hold clues about [who the killers](#) — Farook and his wife, Tashfeen Malik — communicated with while planning the shootings and about where they traveled before and after the attack. Investigators are still working to piece together what happened during 18 minutes on Dec. 2, between the time of the attacks and the moment they were killed in a police shootout.

• Why are Apple phones hard to crack?

Law enforcement officials have long complained about their inability to access the encrypted contents of smartphones used by suspects. Apple has encrypted the contents of its iPhones since 2014, and only those who know a user's pass code — which federal officials do not, in this case — can access the data. Before 2014, Apple could use an extraction tool that would physically plug into the phone to respond to search warrant requests.

• How's Apple to help?

The judge's [order](#) forces Apple to create and supply highly specialized software that the FBI can load onto an iPhone 5C, the model used by the terrorist. That software would bypass a self-destruct feature that erases the phone's data after too many unsuccessful attempts to guess the passcode.

The FBI wants to be able to try different combinations in rapid sequence until it finds the right one, asking it to remove the tamper resistant hardware that creates an 80th of a millisecond wait time per password attempt. Security experts say the wait time can quickly add up if the FBI attempts hundreds of pass codes at one time. Lastly, the order requires Apple create a tool that could be plugged into the phone to allow the FBI to extract the information.

Associated Press contributed to this report.

URL: <http://www.dailybulletin.com/general-news/20160217/why-are-apple-phones-hard-to-crack>



SAN BERNARDINO SHOOTING: Last hospitalized victim remains in good condition

By [ALEJANDRA MOLINA](#)

2016-02-17 18:38:53

VICTIM IN GOOD CONDITION

The last hospitalized victim of the 22 injured in the Dec. 2 San Bernardino mass shooting remained in a rehabilitation facility on the Loma Linda University East Campus, hospital spokeswoman Briana Pastorino said Wednesday, Feb. 17.

The center has four designations for a patient's health – good, fair, serious and critical. This patient, whose name has not been released, was for a long while in critical condition.

HOW TO HELP

The San Bernardino United Relief Fund has raised \$2.37 million.

To donate directly to the relief fund: Text "SBUNITED" to 71777 or visit arrowheadunitedway.org.

A GoFundMe account set up for the victims by San Bernardino Mayor Carey Davis had raised \$127,412 as of Tuesday, Feb. 9.

To donate: gofundme.com/supportsb

RECOGNIZING FIRST RESPONDERS

The San Bernardino Republican Women Federated is honoring law enforcement leaders who responded to the terror attack at An Evening of Appreciation on Thursday, Feb. 18.

San Bernardino Police Chief Jarrod Burguan, San Bernardino County Sheriff John McMahon, and David Bowdich, assistant director in charge of the FBI's Los Angeles field office, will be recognized.

The 6 p.m. event is at Shandin Hills Golf Club, 3380 Little Mountain Drive, San Bernardino. Tickets are \$16, including dinner.

Their leadership should be recognized at the community level, said Karen Contreras, president of the San Bernardino Republican Women Federated.

Contact the writer: 951-368-9462 or amolina@pe.com

© Copyright 2016 Freedom Communications. All Rights Reserved.
[Privacy Policy](#) | [User Agreement](#) | [Site Map](#)

